

ARTIFICIAL INTELLIGENCE ACCEPTABLE USE POLICY

Artifact 11 to The Future of Third-Party Risk Management & Data Privacy

Organization: [ORGANIZATION LEGAL NAME]

Policy Owner: [TITLE OF ACCOUNTABLE EXECUTIVE]

Version: 1.0 | Effective: [DATE] | Review Cycle: Annual

Framework alignment: NIST AI RMF 1.0 and NIST AI 600-1 | ISO/IEC 42001:2023

INTERNAL

 **GUIDANCE:** *This is a model policy, not a finished one. Bracketed placeholders mark every decision the adopting organization must make for itself. The posture throughout is permissive with guardrails: broad permission to use approved tools, bounded tightly by data classification. That posture is deliberate. Survey evidence consistently shows that restrictive policies do not reduce AI use, they relocate it into personal accounts where nothing is logged and nothing is recoverable. A policy that adds prohibitions without funding a fast, credible sanctioned path changes the paperwork and not the behavior.*

SECTION 1 – PURPOSE, SCOPE, AND APPLICABILITY

- 1.1 This Artificial Intelligence Acceptable Use Policy (the "Policy") establishes the conditions under which personnel of [ORGANIZATION] may use artificial intelligence (AI) tools in the course of their work. Its purpose is to enable the productive use of AI while protecting confidential information, personal data, intellectual property, and the accuracy of work product issued in [ORGANIZATION]'s name.
- 1.2 This Policy applies to all employees, officers, contractors, consultants, temporary staff, interns, and any other person performing work for or on behalf of [ORGANIZATION] (collectively, "Personnel"), regardless of location, employment status, or whether the work is performed on [ORGANIZATION]-issued or personal equipment.
- 1.3 This Policy applies to any AI System, whether: (a) publicly available; (b) licensed by [ORGANIZATION]; (c) embedded within software [ORGANIZATION] already uses; (d) developed internally; or (e) provided by a third party in the course of delivering services to [ORGANIZATION]. Applicability is determined by the function performed, not by the product name or the vendor.
- 1.4 This Policy supplements and does not replace [ORGANIZATION]'s Information Security Policy, Acceptable Use Policy, Data Classification Standard, Privacy Policy, Code of Conduct, and Record Retention Policy. Where this Policy and another [ORGANIZATION] policy conflict, the more protective requirement applies.
- 1.5 [ORGANIZATION] permits and encourages the use of Approved AI Tools within the boundaries set out in this Policy. Personnel are not required to seek permission for each individual task. Personnel are required to use approved tools, respect the data handling rules in Section 7, and remain accountable for their output under Section 8.

 **GUIDANCE:** *Clause 1.3 is the most commonly omitted scope provision and the one Personnel most*

reasonably read as permitting. AI embedded inside software the organization has already approved, a meeting transcription feature, a summarization button in a customer relationship management system, an assistant inside a productivity suite, is AI use. Defining scope by function rather than by product name is also what keeps the Policy alive as tools change. Clause 1.5 is the posture statement. Removing it converts this document into a default-deny policy and the guidance throughout the remainder should then be re-read accordingly.

SECTION 2 – DEFINITIONS

"AI System" means a machine-based system that, for explicit or implicit objectives, infers from the input it receives how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.

"Generative AI" means an AI System that produces text, code, images, audio, video, or other content in response to a prompt.

"AI Agent" means an AI System that plans and executes a sequence of actions toward a goal with limited or no human intervention at each step, including systems that can call tools, access systems, send communications, or initiate transactions. "Agentic AI" is used interchangeably.

"Approved AI Tool" means an AI System listed on the AI Tools Register as approved for use, at the account type and data tier specified in that entry.

"AI Tools Register" means the maintained record of Approved AI Tools, Prohibited AI Tools, and AI Agents described in Section 4, published at [LOCATION].

"Shadow AI" means any use of an AI System for [ORGANIZATION] work that is not through an Approved AI Tool and account type, including use of a personal account to access a tool that is approved at the enterprise tier.

"Enterprise Instance" means an AI System accessed through an account provisioned and administered by [ORGANIZATION], under commercial terms that exclude [ORGANIZATION] data from provider model training and support administrative logging and retention control.

"Consumer Instance" means any free, personal, or individually purchased account for an AI System, including the free tier of a product that [ORGANIZATION] licenses at the enterprise tier.

"Input" means any data, file, prompt, document, image, code, or other material submitted to an AI System, whether by upload, integration, application programming interface, or copy and paste.

"Output" means any content, recommendation, classification, score, or decision produced by an AI System.

"Material Decision" means a decision that affects a person's employment, compensation, access to a service, creditworthiness, legal position, health, or safety, or that commits [ORGANIZATION] to a financial or contractual obligation exceeding [THRESHOLD].

"Human in the Loop" means a named individual with the authority, information, and time to review, override, or reject an Output before it takes effect.

"Non-Human Identity" means a credential, service account, token, or certificate issued to a system or AI Agent rather than to a person.

"Data Tier" means a classification level under [ORGANIZATION]'s Data Classification Standard, as mapped to permitted AI use in Appendix A.

 **GUIDANCE:** *Define AI functionally and the Policy survives the next product cycle. Define it by naming ChatGPT, Copilot, and Gemini and the Policy is obsolete within a quarter and, worse, invites the argument that anything unnamed is unrestricted. The Enterprise Instance and Consumer Instance distinction is the operative one*

in practice: most leakage is not use of a forbidden tool, it is use of an approved tool through the wrong account.

SECTION 3 – GOVERNANCE AND ACCOUNTABILITY

- 3.1 [TITLE OF ACCOUNTABLE EXECUTIVE] owns this Policy and is accountable for its implementation, interpretation, and enforcement.
- 3.2 [ORGANIZATION] shall maintain an AI Governance Committee with representation from, at minimum: information security, privacy or data protection, legal, human resources, and the business functions with the highest AI adoption. The Committee shall meet at least quarterly and shall be responsible for the AI Tools Register, tool approvals, exception decisions, and periodic review of this Policy.
- 3.3 Roles and responsibilities under this Policy shall be documented in a responsibility assignment matrix covering, at minimum: tool approval, security review, privacy review, contract review, training delivery, monitoring, and incident response.
- 3.4 [ORGANIZATION] aligns its AI governance to the NIST AI Risk Management Framework 1.0 and the NIST Generative AI Profile (NIST AI 600-1), cross-referenced to ISO/IEC 42001:2023 as set out in Appendix B. Control language in this Policy shall be traceable to that mapping.
- 3.5 Any Personnel may request an exception to this Policy by submitting a written request to [EXCEPTION MAILBOX] describing the intended use, the data involved, the business justification, and the proposed compensating controls. Exceptions shall be decided by the AI Governance Committee, documented, time-limited to no more than [12] months, and reviewed at expiry.
- 3.6 The absence of a rule in this Policy shall not be interpreted as permission for a use that would breach [ORGANIZATION]'s confidentiality obligations, privacy obligations, professional obligations, or contractual commitments.

 **GUIDANCE:** *Clause 3.4 matters more than it appears to. Framework alignment is no longer purely a credibility exercise. The Texas Responsible Artificial Intelligence Governance Act, effective 1 January 2026, provides affirmative defenses for organizations that discover violations through internal testing and that adhere to a recognized AI risk management framework, naming the NIST AI RMF. Alignment that was previously reputational is now, in at least one jurisdiction, legally operative. Clause 3.5 exists because a policy with no exception route generates undocumented exceptions.*

SECTION 4 – APPROVED AI TOOLS AND REQUEST PROCESS

- 4.1 [ORGANIZATION] shall maintain and publish the AI Tools Register at [LOCATION]. For each entry, the Register shall record: (a) the tool name and provider; (b) the approved account type; (c) the highest Data Tier permitted as Input; (d) the approved use cases and any conditions; (e) the business owner; and (f) the date of last review. The Register shall be reviewed at least quarterly.
- 4.2 Where [ORGANIZATION] licenses an Enterprise Instance of a tool, Personnel shall use that instance. Use of a Consumer Instance of the same tool for [ORGANIZATION] work is prohibited, irrespective of the data involved.
- 4.3 Personnel may request the addition of a tool to the Register by submitting a request to [REQUEST CHANNEL]. [ORGANIZATION] shall acknowledge the request within [2] business days and shall return a decision, a conditional approval, or a written explanation of what is outstanding within [10] business days of receiving the information required for review.

- 4.4 Where a tool is under review, the AI Governance Committee may grant provisional approval limited to Data Tier [PUBLIC] Input, for a period not exceeding [60] days, to allow evaluation without creating an incentive to proceed unapproved.
- 4.5 AI functionality embedded within software already approved by [ORGANIZATION] is not automatically approved. Personnel shall not enable AI features in existing software without confirming the feature appears on the Register. [ORGANIZATION] shall assess embedded AI features as part of the quarterly Register review and shall record each material feature explicitly.
- 4.6 Personnel shall not use a personal account, personal payment method, or personal subscription to obtain AI functionality for [ORGANIZATION] work, and shall not expense such a subscription other than through the process in clause 4.3.

 **GUIDANCE:** *Clause 4.3 is the clause that determines whether this Policy works. The dominant reason Personnel use unapproved tools is not defiance, it is that the sanctioned path is slower than the deadline. A published turnaround commitment converts the Policy from a prohibition into a service. If the organization cannot honor the stated interval, lengthen the interval rather than omitting it. An unmet commitment is more corrosive than a modest one. Clause 4.4 exists for the same reason: an evaluation route that costs nothing is cheaper than the shadow deployment it displaces.*

SECTION 5 – PERMITTED USE

- 5.1 Subject to Sections 6 through 9, Personnel may use Approved AI Tools for [ORGANIZATION] work without seeking task-by-task permission.
- 5.2 Permitted uses include, by way of example and not limitation:
- Drafting, editing, summarizing, translating, and restructuring text that the Personnel member then reviews and adopts as their own work.
 - Research, ideation, outlining, and exploration of alternative approaches.
 - Writing, reviewing, explaining, testing, and documenting code, subject to clause 10.3.
 - Analyzing, transforming, and visualizing data at the Data Tiers permitted in Appendix A.
 - Preparing meeting notes, agendas, and internal correspondence.
 - Learning, skills development, and evaluation of AI capability.
- 5.3 [ORGANIZATION] shall maintain an evaluation environment at [LOCATION] in which Personnel may test Approved AI Tools using synthetic or Tier [PUBLIC] data without further approval.
- 5.4 Time spent developing AI capability in accordance with this Policy is treated as working time and is encouraged.

 **GUIDANCE:** *A permitted-use section is not decorative. Two of the most cited reasons Personnel conceal AI use are that they believe the policy is restrictive and that they do not know whether their particular use is allowed. Ambiguity, not defiance, accounts for a meaningful share of shadow AI. Naming permitted uses explicitly recovers usage into visible channels more effectively than any additional prohibition suppresses it.*

SECTION 6 – PROHIBITED USES

- 6.1 Personnel shall not use any AI System to:
- Make or materially determine a decision regarding hiring, promotion, discipline, termination, compensation, or performance rating, other than as expressly permitted under clause 6.2.

- Reach a legal, medical, financial, tax, or safety determination that is issued or relied upon without review by a qualified person accountable for that determination.
 - Monitor, evaluate, profile, or infer characteristics of individual colleagues, other than through systems formally approved for that purpose by [ORGANIZATION].
 - Generate content that impersonates a real person, including synthetic voice, likeness, or signature, other than with that person's documented consent and for a use approved in advance.
 - Produce material that is discriminatory, harassing, defamatory, or otherwise in breach of [ORGANIZATION]'s Code of Conduct.
 - Circumvent, disable, or evade [ORGANIZATION]'s security, monitoring, data loss prevention, or access controls, including by routing work through personal devices or accounts.
 - Process Input in breach of the Data Tier limits in Appendix A.
 - Access a tool listed as prohibited on the AI Tools Register.
- 6.2 Where AI is used at any stage of a personnel decision process, including screening, ranking, scheduling, or drafting an assessment, the tool shall have been assessed for discriminatory effect before deployment, a Human in the Loop shall make the decision, records shall be retained in accordance with [RECORD RETENTION POLICY], and any notice or accommodation obligations applicable in the relevant jurisdiction shall be met.
- 6.3 Personnel who become aware of a prohibited use, whether their own or another's, shall report it under Section 14.

 **GUIDANCE:** *Separate prohibited tools from prohibited uses and keep them in different places. A tool list changes monthly and belongs in the Register. Prohibited uses are categorical and belong in the Policy. Clause 6.2 carries real legal weight in the United States: Illinois House Bill 3773, effective 1 January 2026, amends the Illinois Human Rights Act to prohibit employer use of AI that discriminates against protected classes, and California's Civil Rights Council regulations on automated decision systems, effective 1 October 2025, impose anti-discrimination, recordkeeping, and third-party accountability duties on employers. Both attach to the employer as deployer, regardless of which vendor built the tool.*

SECTION 7 – DATA HANDLING AND CLASSIFICATION

- 7.1 Permitted Input is determined by Data Tier. Appendix A sets out the mapping between [ORGANIZATION]'s Data Classification Standard and permitted AI use, with worked examples for each tier. Personnel shall classify Input before submitting it.
- 7.2 Copying and pasting text into an AI System is a disclosure of that text and is governed by the same rules as uploading a file. Screenshots, pasted tables, and transcribed audio are likewise Input.
- 7.3 Removing names is not sufficient to reduce the Data Tier of Input. Personnel shall not treat data as de-identified unless it has been processed in accordance with [ORGANIZATION]'s de-identification standard and the residual re-identification risk has been assessed.
- 7.4 Client, customer, and counterparty information held under contract shall not be submitted to any AI System unless the applicable agreement permits it, or the client has given documented consent. Where a client agreement is silent on AI, Personnel shall treat AI submission as requiring consent and shall refer the question to [LEGAL CONTACT].
- 7.5 Personal data shall be submitted to an AI System only where a lawful basis exists, the processing is within the scope of the relevant privacy notice, and any required assessment has been completed. Special category data shall not be submitted without prior approval from [PRIVACY CONTACT].

- 7.6 Personnel shall not use an AI System whose terms permit the provider to use [ORGANIZATION] Input to train, fine-tune, or improve its models, other than for Tier [PUBLIC] Input. The AI Tools Register shall record the training-use position for each entry.
- 7.7 Conversation history, uploaded files, and generated Outputs held within an AI System are [ORGANIZATION] records where they relate to [ORGANIZATION] business, and are subject to [RECORD RETENTION POLICY] and to legal hold. Personnel shall not delete such material where a hold is in force.

 **GUIDANCE:** *Clause 7.2 exists because most Personnel do not experience pasting as transmitting data. Browser telemetry consistently identifies copy and paste, not file upload, as the dominant path by which corporate data leaves enterprise control. Say it in the Policy, then reinforce it in training, because the intuition runs the other way. Clause 7.4 is the third-party risk clause hiding inside an internal policy: an engagement letter that predates generative AI almost certainly does not contemplate submission of client material to a model provider, and silence is not permission. Clause 7.7 is routinely omitted and then discovered during the first litigation hold.*

SECTION 8 – HUMAN ACCOUNTABILITY AND VERIFICATION

- 8.1 The Personnel member who submits, publishes, sends, or relies on work product owns that work product in full, whether or not an AI System assisted in producing it. AI assistance does not transfer, dilute, or share responsibility for accuracy, quality, or compliance.
- 8.2 Before AI-assisted work product leaves the hands of the Personnel member who prepared it, that person shall independently verify:
- Every factual assertion, against a source they have examined.
 - Every citation, quotation, case reference, statutory reference, and standard reference, against the original.
 - Every calculation, figure, and data point.
 - Every name, date, title, and attribution.
 - For code, that it functions as intended, introduces no known vulnerability, and carries no incompatible license.
- 8.3 An Output shall not be the sole basis for a Material Decision. A Human in the Loop shall review the Output, be able to explain the basis for the decision without reference to the AI System's reasoning, and have the authority to reject it.
- 8.4 Personnel holding a professional license, certification, or regulatory registration remain bound by the standards of that profession, which are not modified by this Policy and which may impose stricter verification or disclosure duties.
- 8.5 Personnel shall not submit AI-generated material to a client, regulator, court, auditor, or public forum without completing the verification required by clause 8.2.

 **GUIDANCE:** *This is the clause that addresses the failure mode most likely to cause visible damage. In October 2025 Deloitte Australia agreed to partially refund a A\$440,000 assurance engagement for the Department of Employment and Workplace Relations after its report was found to contain fabricated quotations from federal court rulings and citations to academic papers that do not exist. Nothing leaked. The controls that would have prevented it are in clause 8.2, not in a data loss prevention rule. Note also that a majority of employees report relying on AI output without evaluating its accuracy, which means the verification duty must be stated as a procedure, not as an expectation of good judgment.*

SECTION 9 – DISCLOSURE AND ATTRIBUTION

- 9.1 Personnel shall disclose AI assistance where the Output is substantive rather than assistive. Substantive use means the AI System generated the analysis, the conclusion, the structure, or the substantial majority of the content. Assistive use means editing, formatting, summarizing the Personnel member's own material, translation, or spelling and grammar correction, and does not require disclosure.
- 9.2 Disclosure is required in all cases, regardless of the assistive or substantive distinction, for: (a) deliverables issued to a client where the engagement terms require it; (b) submissions to a regulator, court, or auditor; (c) published research, thought leadership, and marketing claims; (d) any deliverable where a person's reliance on the Output could cause harm; and (e) any case where a client, counterparty, or regulator has asked.
- 9.3 Where disclosure is required, it shall identify that AI was used, in what role, and that the Output was reviewed by a named human. [ORGANIZATION] shall publish standard disclosure wording at [LOCATION].
- 9.4 Personnel shall not present AI-generated work as unaided human work where clause 9.1 or 9.2 requires disclosure, and shall not conceal AI use in response to a direct question.
- 9.5 Personnel shall not falsely claim that a deliverable was AI-generated in order to disclaim responsibility for it.

 **GUIDANCE:** *More than half of employees report hiding their AI use and presenting AI-generated work as their own. That figure should be read as a design failure rather than an integrity failure: where a policy is silent on disclosure, concealment is the rational default because disclosure carries perceived career cost and no perceived benefit. The assistive and substantive distinction in clause 9.1 is what makes the rule followable. A blanket disclosure requirement for any AI touch produces disclosure fatigue and then non-compliance. Set the threshold where it means something.*

SECTION 10 – INTELLECTUAL PROPERTY AND LICENSING

- 10.1 As between [ORGANIZATION] and Personnel, [ORGANIZATION] owns all work product created using AI Systems in the course of employment or engagement, to the extent such rights are capable of ownership.
- 10.2 Personnel acknowledge that the copyright status of material generated substantially by AI is unsettled in several jurisdictions and that such material may not be protectable. Personnel shall consult [LEGAL CONTACT] before relying on AI-generated material as a protectable asset, filing for registration, or asserting exclusivity.
- 10.3 AI-generated or AI-assisted code shall be reviewed by a qualified person before merge, scanned for known vulnerabilities and for license compatibility, and recorded such that its origin can be traced. AI-generated code shall not be committed to a repository governed by a license whose obligations have not been assessed.
- 10.4 Personnel shall not submit third-party intellectual property, including licensed content, competitor material, or material subject to a non-disclosure agreement, as Input, other than where the applicable license or agreement permits it.
- 10.5 Personnel shall not use an AI System to reproduce, imitate, or derive from a third party's distinctive protected expression, trade dress, or trademarked material.

SECTION 11 – AGENTIC AND AUTONOMOUS AI

- 11.1 No AI Agent shall be deployed in [ORGANIZATION]'s environment, or granted access to [ORGANIZATION] systems, data, communications, or funds, without prior security review and approval by [SECURITY FUNCTION] and registration on the AI Tools Register.
- 11.2 Every AI Agent shall have a named human owner who is accountable for its behavior, its access, and its outcomes, and a named deputy. Accountability shall not be assigned to a team or a mailbox.
- 11.3 Every AI Agent shall operate under a distinct Non-Human Identity, provisioned under least privilege, with credentials rotated on the schedule in [CREDENTIAL STANDARD], and shall not share, inherit, or assume the credentials of a human user.
- 11.4 The approved scope of each AI Agent shall be documented before deployment and shall state: the systems it may access; the actions it may take without human confirmation; the actions requiring human confirmation; the financial or transactional limits that apply; and the conditions under which it must stop and escalate.
- 11.5 Every action taken by an AI Agent shall be logged to [LOG DESTINATION] with sufficient detail to reconstruct what it did, on whose behalf, and on what basis. Logs shall be retained in accordance with [RECORD RETENTION POLICY] and shall be tamper-evident.
- 11.6 Every AI Agent shall have a documented and tested method of immediate suspension. [ORGANIZATION] shall test the suspension of each production AI Agent at least [annually], shall record the elapsed time to full suspension, and shall treat a failure to suspend within [TARGET] as a security incident.
- 11.7 AI Agents shall not invoke, instruct, or delegate to other AI Agents outside their approved scope without a further review under clause 11.1.
- 11.8 An AI Agent shall not take a Material Decision. Where an AI Agent's action would constitute or trigger a Material Decision, it shall stop and escalate to its named owner.

 **GUIDANCE:** *This section is the newest and the least mature in most organizations, which is precisely why it belongs in version 1.0 rather than a later revision. The gap is quantified: in the ISACA 2026 AI Pulse Poll, 39 percent of respondents reported no documented process for shutting down an AI system and 56 percent did not know how long a shutdown would take. Clause 11.6 turns that from an assumption into a tested control with a recorded time, which is the form an auditor can examine. Clause 11.3 is the identity clause: an agent operating under a human's credentials is invisible in the access review, indistinguishable in the log, and impossible to revoke without locking out the person.*

SECTION 12 – THIRD-PARTY AND VENDOR AI

- 12.1 [ORGANIZATION] shall require each material vendor to notify [ORGANIZATION] before introducing AI into a service already under contract, and to maintain an inventory of AI Systems used in delivering that service. The contractual mechanism is set out in [Artifact 10, Section 15].
- 12.2 Personnel shall not introduce [ORGANIZATION] data into a vendor's AI functionality that has not been assessed under [ORGANIZATION]'s third-party risk management process, irrespective of whether the underlying vendor relationship is approved.
- 12.3 Vendor AI assessments shall consider fourth-party model providers and subprocessors, the vendor's own acceptable use policy for its personnel, its controls against Shadow AI, and its position on training with client data.

- 12.4 Procurement of any product or service with material AI functionality shall route through [PROCUREMENT GATE] before contract execution, and the AI Governance Committee shall be a required reviewer.

 **GUIDANCE:** *This is the section that connects the internal policy to the third-party risk program, and it is the one most internal-only AI policies omit entirely. The asymmetry is worth naming to the business: organizations that require vendors to hold an AI acceptable use policy, to maintain an approved tools list, and to train their staff, while not doing those things themselves, lose that position the first time a client sends them the same questionnaire.*

SECTION 13 – TRAINING AND AI LITERACY

- 13.1 All Personnel shall complete AI acceptable use training within [30] days of hire or engagement, before being granted access to any Approved AI Tool.
- 13.2 All Personnel shall complete refresher training at least annually, and additional training within [30] days of any material amendment to this Policy or the AI Tools Register.
- 13.3 Training shall be role-differentiated. At minimum, [ORGANIZATION] shall provide: a general module for all Personnel; an extended module for Personnel handling client data, personal data, or regulated data; a technical module for Personnel building, integrating, or operating AI Systems or AI Agents; and a governance module for Personnel with approval or oversight responsibilities.
- 13.4 Training shall cover, at minimum: what is permitted; the Data Tier rules and worked examples; the verification duty under Section 8; the disclosure rules under Section 9; how to request a tool; how to report a concern; and the consequences of non-compliance.
- 13.5 [ORGANIZATION] shall retain records of training completion sufficient to demonstrate compliance to a regulator, client, or auditor.
- 13.6 Where [ORGANIZATION] deploys AI Systems with a nexus to the European Union, training shall be designed to meet the AI literacy obligation on deployers under Article 4 of Regulation (EU) 2024/1689, taking into account the technical knowledge, experience, education, and training of the Personnel concerned and the context in which the AI Systems are used.

 **GUIDANCE:** *Article 4 of the EU AI Act has applied since 2 February 2025 and binds deployers, not only providers. It is a competence obligation rather than a disclosure obligation, which means an acknowledgment form does not satisfy it and a single generic module for the whole workforce is difficult to defend, since the Article expressly requires calibration to the role and context. Clause 13.3 is drafted to meet that calibration requirement. Note also that only about a third of organizations currently train all employees on AI, so this section is where most programs are furthest from their own stated policy.*

SECTION 14 – MONITORING, REPORTING, AND ENFORCEMENT

- 14.1 [ORGANIZATION] monitors the use of AI Systems on its networks, devices, and accounts. Monitoring may include [network and web traffic inspection; data loss prevention on endpoints, email, and browsers; browser extension telemetry; administrative logs within Enterprise Instances; and discovery of unsanctioned applications]. [ORGANIZATION] does not monitor [PERSONAL DEVICE / PERSONAL ACCOUNT SCOPE EXCLUSIONS].
- 14.2 Monitoring is carried out under [LEGAL BASIS] and is described in [EMPLOYEE PRIVACY NOTICE]. Where local law or a works council agreement requires consultation, notice, or agreement before monitoring, [ORGANIZATION] shall complete that process before deploying the monitoring in that jurisdiction.

- 14.3 For a period of [90] days from the effective date of this Policy, Personnel may disclose prior or current use of an unapproved AI System, or a prior disclosure of data to an AI System, without disciplinary consequence, provided the disclosure is complete and made before [ORGANIZATION] identifies the use independently. The purpose of this clause is to establish an accurate inventory.
- 14.4 Personnel shall report the following to [REPORTING CHANNEL] within [24] hours of becoming aware: a disclosure of data to an AI System in breach of Section 7; an Output error that has reached a client, regulator, or the public; an AI Agent acting outside its approved scope; a suspected compromise of an AI System or Non-Human Identity; and any AI-related matter that would be reportable under [INCIDENT RESPONSE PLAN].
- 14.5 [ORGANIZATION] shall not retaliate against Personnel for a good-faith report under this Policy, including a report concerning a colleague or a member of management.
- 14.6 Violations of this Policy may result in disciplinary action up to and including termination, and in the case of contractors, termination of engagement. This Policy applies equally to all Personnel at every level, including executive management, and enforcement shall be recorded so that consistency can be demonstrated.
- 14.7 This Policy shall be reviewed at least annually by the AI Governance Committee, and additionally upon a material change in [ORGANIZATION]'s AI use, a material change in applicable law, or a significant AI-related incident. Jurisdiction-specific obligations shall be maintained in Appendix D so that they can be updated without reissuing the body of the Policy.

 **GUIDANCE:** Clause 14.6 addresses the most damaging perception in the survey data: among employees who believe their organization has an AI policy, a large majority believe it is enforced more strictly against staff than against leadership. Uneven enforcement does not merely fail to deter, it actively teaches Personnel that concealment is the correct strategy. Clause 14.3 is the amnesty provision and it is the single highest-value clause at rollout. Organizations that issue an AI policy without one inherit an unmeasured shadow inventory and never learn its size. Clause 14.1 should be edited down to what the organization genuinely operates. A monitoring clause describing controls that do not exist is worse than no clause, because it is discoverable.

APPENDIX A – DATA CLASSIFICATION AND PERMITTED AI USE

Map this table to [ORGANIZATION]'s existing Data Classification Standard. Tier names below are illustrative and should be replaced with the organization's own. Worked examples are mandatory, not optional: Personnel classify in the moment, under time pressure, and cannot apply an abstract definition.

Data Tier	Approved Enterprise Instance	Consumer Instance	Worked examples
Tier 1 – Public	Permitted	Permitted for evaluation only	Published marketing copy, public regulatory text, information already on the website, synthetic test data.
Tier 2 – Internal	Permitted	Prohibited	Internal process documentation, meeting agendas, non-sensitive project plans, draft internal communications.
Tier 3 – Confidential	Permitted only for the tools flagged Tier 3 on the Register	Prohibited	Vendor contracts, risk assessments, internal financial analysis, unpublished strategy, employee names in a business context.

Tier 4 – Restricted	Prohibited absent an approved exception under clause 3.5	Prohibited	Client data held under contract, personal data of customers or employees, special category data, credentials and keys, material non-public information, privileged legal material, source code for [NAMED SYSTEMS].
---------------------	--	------------	---

APPENDIX B – FRAMEWORK CROSS-WALK

Mapping of this Policy to the NIST AI Risk Management Framework 1.0 functions and to the ISO/IEC 42001:2023 Annex A control groups. Use this table to answer client and auditor questionnaires without re-deriving the mapping each time.

Policy section	NIST AI RMF function	ISO/IEC 42001:2023 Annex A group
1 Purpose and scope	GOVERN	A.2 Policies related to AI
2 Definitions	MAP	A.2 Policies related to AI
3 Governance and accountability	GOVERN	A.3 Internal organisation; A.4 Resources for AI systems
4 Approved tools and requests	GOVERN; MAP	A.4 Resources for AI systems; A.6 AI system life cycle
5 Permitted use	GOVERN	A.9 Use of AI systems
6 Prohibited uses	MAP; MANAGE	A.5 Assessing impacts of AI systems; A.9 Use of AI systems
7 Data handling	MAP; MANAGE	A.7 Data for AI systems
8 Human accountability	MEASURE; MANAGE	A.9 Use of AI systems
9 Disclosure and attribution	GOVERN; MEASURE	A.8 Information for interested parties
10 Intellectual property	GOVERN	A.6 AI system life cycle
11 Agentic and autonomous AI	MAP; MEASURE; MANAGE	A.6 AI system life cycle; A.9 Use of AI systems
12 Third-party and vendor AI	GOVERN; MAP	A.10 Third-party and customer relationships
13 Training and AI literacy	GOVERN	A.4 Resources for AI systems
14 Monitoring and enforcement	MEASURE; MANAGE	A.6 AI system life cycle; A.8 Information for interested parties

 **GUIDANCE:** ISO/IEC 42001:2023 contains 38 Annex A controls across nine groups, A.2 through A.10. The mapping above is to the group level deliberately. Mapping a policy to individual controls invites a false precision that does not survive an audit, because a single policy clause rarely satisfies a control on its own. Add the control-level detail in the Statement of Applicability, where it belongs, and keep the Policy mapped at the group level.

APPENDIX C – ACKNOWLEDGMENT

I confirm that I have read and understood [ORGANIZATION]'s Artificial Intelligence Acceptable Use Policy. I understand that I remain fully accountable for any work product I produce with the assistance of an AI System, that I am required to verify its accuracy before it leaves my hands, and that I am required to

use only Approved AI Tools through the account type specified in the AI Tools Register. I understand that violations may result in disciplinary action up to and including termination.

Name	Signature	Date

APPENDIX D – JURISDICTIONAL OBLIGATIONS

Maintained separately from the body of this Policy so that it can be revised without reissuing the Policy. Complete for each jurisdiction in which [ORGANIZATION] has Personnel or deploys AI Systems. Confirm current status with counsel before issue: the state and national picture is moving quickly, and at least one significant statute, the Colorado AI Act, was repealed and replaced during 2026.

Jurisdiction	Instrument	Obligation on [ORGANIZATION] as deployer	Status
European Union	Regulation (EU) 2024/1689, Article 4	Ensure a sufficient level of AI literacy among staff and others operating AI on the organization's behalf, calibrated to role and context.	Applies since 2 Feb 2025
California	Civil Rights Council automated decision system regulations	Anti-discrimination, recordkeeping, and third-party accountability duties where automated decision systems are used in employment decisions.	Effective 1 Oct 2025
Illinois	House Bill 3773 (P.A. 103-0804)	Prohibits employer use of AI that discriminates against protected classes; notice obligations apply.	Effective 1 Jan 2026
Texas	Responsible Artificial Intelligence Governance Act	Prohibits AI use for restricted purposes; affirmative defenses available for internal testing and recognized framework adherence.	Effective 1 Jan 2026
Colorado	SB 26-189, Automated Decision-Making Technology Act	Replaced the Colorado AI Act. Narrower transparency duties around adverse automated outcomes; no duty of reasonable care.	Signed 14 May 2026; effective 1 Jan 2027
[OTHER]	[INSTRUMENT]	[OBLIGATION]	[STATUS]

Artifact 11 to The Future of Third-Party Risk Management & Data Privacy. This model policy is provided for adaptation and does not constitute legal advice. Confirm all jurisdiction-specific obligations with counsel before issue.